

Appl. No. 09/895,692  
Amdt. Dated: 01/10/2005  
Reply to Office Action of 08/10/2004

RECEIVED  
JAN 10 2005

**Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1           1.       (Currently Amended) A state-varying hybrid stream cipher operating within a  
2 computing device, comprising:  
3           a first software routine to divide incoming plain text into variable-sized blocks with each  
4 block varying in size; and  
5           a second software routine to convert the plain text into cipher text based on an encryption  
6 key, an internal identifier and an internal state of the computing device.

1           2.       (Original) The state-varying hybrid stream cipher of claim 1, wherein the first  
2 software routine produces the variable-sized blocks based on the encryption key, the internal  
3 identifier and an output of a first non-linear function.

1           3.       (Original) The state-varying hybrid cipher of claim 2, wherein each current block  
2 of the plain text is determined by (i) producing a pseudo-random sequence using a second non-  
3 linear function including the encryption key, the internal identifier and the output of the first non-  
4 linear function as inputs and (ii) accessing contents of the pseudo-random sequence as a number  
5 of data elements of the plain text forming the current block.

1           4.       (Original) The state-varying hybrid cipher of claim 1 further comprising:  
2           a third software routine to determine if a plurality of random data elements are to be  
3 distributed within the cipher text and to compute a hash digest of the random data elements.

1           5.       (Original) The state-varying hybrid cipher of claim 4 further comprising a fourth  
2 software routine to perform a first shuffling operation on the internal state of the computing  
3 device based on the encryption key so that a single bit modification of the encryption key

Appl. No. 09/895,692  
Amdt. Dated: 01/10/2005  
Reply to Office Action of 08/10/2004

4 requires complete recalculation of the internal state of the computing device used to encrypt the  
5 random data elements.

1 6. (Original) The state-varying hybrid cipher of claim 4, wherein the second  
2 software routine further performs a second shuffling operation on the internal state of the  
3 computing device prior to encrypting the random data elements based on the encryption key and  
4 the internal identifier to mitigate a likelihood of prediction of the internal state of the computing  
5 device upon knowledge of the encryption key.

1 7. (Original) The state-varying hybrid cipher of claim 4, wherein the third software  
2 routine determines a statistical amount of random data elements distributed within the cipher text  
3 is programmable based on a percentage value entered by a user.

1 8. (Original) The state varying hybrid cipher of claim 7, wherein the distribution of  
2 random data elements within the cipher text is based on the encryption key, the internal identifier  
3 and internal state of the computing device.

1 9. (Original) The state-varying hybrid cipher of claim 1 further comprising a third  
2 software routine to distribute error correcting codes in the cipher text in order to correct  
3 modifications.

1 10. (Original) The state-varying hybrid cipher of claim 1, wherein the internal state  
2 of the computing device is periodically modified.

1 11. (Original) The state-varying hybrid cipher of claim 1, wherein the internal state  
2 of the computing device is based on a time value.

1 12. (Currently Amended) A computing device comprising:  
2 a memory; and

Appl. No. 09/895,692  
Amdt. Dated: 01/10/2005  
Reply to Office Action of 08/10/2004

3           logic coupled to the memory, the logic to perform a state-varying stream cipher  
4   operation, controlled by at least an encryption key and an internal state of the computing device,  
5   on input data segmented in random sized blocks using the encryption key.

1           13.   (Original) The computing device of claim 12, wherein the stream cipher  
2   operation involves encryption.

1           14.   (Original) The computing device of claim 12, wherein the logic is an integrated  
2   circuit.

1           15.   (Original) The computing device of claim 12, wherein the internal state of the  
2   computing device varies over time.

1           16.   (Original) The computing device of claim 15, wherein the variation of the  
2   internal state of the computing device is periodic being set at a time that an encryption process  
3   begins for each block of input data.

1           17.   (Currently Amended) The computing device of claim 12, wherein the computing  
2   device is one of a smart card and an operating system.

1           18.   (Currently Amended) The computing device of claim ~~15~~12, wherein the logic of  
2   the computing device ~~is an operating system segmenting the input data into at least three random~~  
3   sized blocks with each block varying in length.

1           19.   (Original) A method for decrypting input data using a combination of stream  
2   cipher and block cipher functionality, comprising:  
3           receiving as input a cipher text, a decryption key, a percentage of random data and a  
4   unique internal identifier; and  
5           reiteratively decrypting blocks of the cipher text using the decryption key, the  
6   percentage of random data, the unique internal identifier and a varying internal state of the  
7   computing device to recover corresponding blocks of plain text.

Appl. No. 09/895,692  
Amdt. Dated: 01/10/2005  
Reply to Office Action of 08/10/2004

- 1           20.    (Original) The method of claim 19, wherein the internal state of the computing
- 2   device varies over continuously over time.